Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	1	"5457748".pn.	USPAT	OR	OFF	2004/03/05 12:01
S2	617	380/28.ccls.	USPAT	OR	OFF	2004/03/01 18:39
S3	679	380/28.ccls. and "random number" "change intermediate"	USPAT	OR	OFF	2004/03/01 18:32
S4	0	380/28.ccls. and "random number" and "change intermediate"	USPAT	OR	OFF	2004/03/01 18:33
S5	5	380/28.ccls. and "random number" and "change data"	USPAT	OR	OFF	2004/03/01 18:33
S6	234	380/28.ccls. and "random number"	USPAT	OR	OFF	2004/03/01 18:34
S7	3	380/28.ccls. and "random number" and "intermediate data"	USPAT	OR	OFF	2004/03/01 18:39
S8	0	380/46.ccls. and "random number" and "intermediate dat"	USPAT	OR	OFF	2004/03/01 18:40
S9	0	380/46.ccls. and "random number" and "intermediate data"	USPAT	OR	OFF	2004/03/01 18:40
S10	235	380/46.ccls. and "random number"	USPAT	OR	OFF	2004/03/01 18:41
S11	154	380/44.ccls. and "random number"	USPAT	OR	OFF	2004/03/01 18:42
S12	145	380/44.ccls. and "random number" and encrypt$8	USPAT	OR	OFF	2004/03/01 18:57
S13	204	380/37.ccls.	USPAT	OR	OFF	2004/03/01 18:57
S14	58	380/37.ccls. and "random number"	USPAT	OR	OFF	2004/03/01 19:33
S15	1	"6157120".pn.	USPAT	OR	OFF	2004/03/01 18:58
S16	1	"6157720".pn.	USPAT	OR	OFF	2004/03/01 18:58
S17	22	380/37.ccls. and "random number" and encrypt$8.ti.	USPAT	OR	OFF	2004/03/01 19:39
S18	5	"380"/$.ccls. and "random number" and encrypt$8.ti. and "intermediate data"	USPAT	OR	OFF	2004/03/01 19:41
S19	45	"380"/$.ccls. and "random number" and encrypt$8.ti. and "delay"	USPAT	OR	OFF	2004/03/01 19:41
S20	75	380/35.ccls.	USPAT	OR	OFF	2004/03/02 11:46
S21	88	380/36.ccls.	USPAT	OR	OFF	2004/03/02 11:46
S22	204	380/37.ccls.	USPAT	OR	OFF	2004/03/02 11:47
S23	165	380/37.ccls. and encryption	USPAT	OR	OFF	2004/03/02 12:20
S24	6464	380/37.ccls. and encryption amd	USPAT	OR	OFF	2004/03/02 12:20

S25	51	380/37.ccls. and encryption and "random number"	USPAT	OR	OFF	2004/03/02 12:34
S26	1229	"380"/$.ccls. and encryption and "random number"	USPAT	OR	OFF	2004/03/02 12:34
S27	229	"380"/$.ccls. and encryption and "random number" and encrypt$.ti.	USPAT	OR	OFF	2004/03/02 12:56
S28	0	(chang$3 or modif$3 or alter$7) near2 "encrypting operation"	USPAT	OR	OFF	2004/03/02 12:59
S29	1043	(chang$3 or modif$3 or alter$7) near2 encrypt$6	USPAT	OR	OFF	2004/03/02 13:00
S30	1	((chang$3 or modif$3 or alter$7) near2 encrypt$6) same (step or stage) same ("random number")	USPAT	OR	OFF	2004/03/02 14:01
S31	134	((chang$3 or modif$3 or alter$7) near2 encrypt$6) same (step or stage)	USPAT	OR	OFF	2004/03/02 13:03
S32	40	((chang$3 or modif$3 or alter$7) near2 encrypt$6) same ("random number")	USPAT	OR	OFF	2004/03/02 13:43
S33	1	"5457748".pn.	USPAT	OR	OFF	2004/03/02 13:53
S34	1	"4969190".pn.	USPAT	OR	OFF	2004/03/02 13:54
S35	1	"4982429".pn.	USPAT	OR	OFF	2004/03/02 13:56
S36	1	"5144665".pn.	USPAT	OR	OFF	2004/03/02 13:56
S37	0	"6683956".URPN.	USPAT	OR	OFF	2004/03/02 13:58
S38	6	("4850019" \| "4926479" \| "5103479" \| "5193115" \| "5270956" \| "5742678").PN.	USPAT	OR	OFF	2004/03/02 14:01
S39	4	((chang$3 or modif$3 or alter$7) near2 encrypt$6) same (step or stage) same ("random number")	US-PGPUB; USPAT; EPO; JPO	OR	OFF	2004/03/02 14:55
S40	1	"6683956".pn.	USPAT	OR	OFF	2004/03/04 18:32
S41	6	("4850019" \| "4926479" \| "5103479" \| "5193115" \| "5270956" \| "5742678").PN.	USPAT	OR	OFF	2004/03/04 18:33
S42	1	"4982429".pn.	USPAT	OR	OFF	2004/03/05 12:02
S43	1	"5218638".pn.	USPAT	OR	OFF	2004/03/05 12:02
S44	1	"5966448".pn.	USPAT	OR	OFF	2004/03/05 12:03
S45	1	"6504931".pn.	USPAT	OR	OFF	2004/03/05 12:05
S46	251	380/43.ccls.	USPAT	OR	OFF	2004/03/05 12:06
S47	62	380/43.ccls. and "random number"	USPAT	OR	OFF	2004/03/05 12:16
S48	30	encrypt$8 and decrypt$8 and "random number" and "intermediate data" and (change$5 same encrypt$8)	USPAT; EPO; JPO	OR	OFF	2004/03/05 12:32

S49	4	encrypt$8 and decrypt$8 and "random number" and "intermediate data" and "work key"	USPAT; EPO; JPO	OR	OFF	2004/03/05 12:35
S50	1	"6122375".pn.	USPAT; EPO; JPO	OR	OFF	2004/03/05 12:33
S51	17	encrypt$8 and decrypt$8 and "random number" and "work key"	USPAT; EPO; JPO	OR	OFF	2004/03/05 14:49
S52	5	"793366"	USPAT; EPO; JPO	OR	OFF	2004/03/05 14:50
S53	1	"6157720".pn.	USPAT	OR	OFF	2004/03/05 15:29
S54	4	("5285497" \| "5351299" \| "5479512" \| "5517614").PN.	USPAT	OR	OFF	2004/03/05 15:30
S55	1	"6157720".URPN.	USPAT	OR	OFF	2004/03/05 15:30
S56	6	("5285497" \| "5351299" \| "5442705" \| "5479512" \| "5517614" \| "6157720").PN.	USPAT	OR	OFF	2004/03/05 15:45
S57	1	"6175850".pn.	USPAT	OR	OFF	2004/03/05 15:47
S58	1	"6408075".pn.	USPAT	OR	OFF	2004/03/05 15:47
S59	5	"6606385".pn. or "6175850".pn. or "6683956".pn. or "601881".pn. or "6125186".pn. or "6125186". pn. or "6157720".pn.	USPAT	OR	OFF	2004/03/10 11:42
S60	6	"6606385".pn. or "6175850".pn. or "6683956".pn. or "6018581". pn. or "6125186".pn. or "6125186".pn. or "6157720".pn.	USPAT	OR	OFF	2004/03/10 12:26
S61	1	"5442705".pn.	USPAT	OR	OFF	2004/03/10 12:26
S62	1	"5835727".pn.	USPAT	OR	OFF	2005/03/11 18:26
S63	1	"6606385".pn.	USPAT	OR	OFF	2005/03/11 18:27
S64	1	"6175850".pn.	USPAT	OR	OFF	2005/03/11 18:27
S65	769	380/28.ccls.	USPAT; EPO; JPO	OR	OFF	2005/06/08 12:30
S67	471	380/44.ccls.	USPAT; EPO; JPO	OR	OFF	2005/06/08 12:30
S68	282	380/37.ccls.	USPAT; EPO; JPO	OR	OFF	2005/06/08 12:30
S69	567	380/46.ccls.	USPAT; EPO; JPO	OR	OFF	2005/06/08 12:30
S70	643	380/46.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/06/08 12:30

S71	976	380/28.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/06/08 12:30
S72	607	380/44.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/06/08 12:30
S73	418	380/37.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/06/08 12:33
S74	28	380/37,44,46,28.ccls. and (power with analysis)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/06/08 12:34
S75	30	380/37,44,46,28.ccls. and ((chang$3 or modif$3 or alter$3) near2 encrypt$6) same (step or stage)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/06/08 12:45
S76	12	380/37,44,46,28.ccls. and (cryptanalysis.ab.)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/06/08 12:45
S77	31	380/37,44,46,28.ccls. and intermediate adj data	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/06/08 12:45
S78	17	380/37,44,46,28.ccls. and (intermediate adj data) same (stage step)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/06/08 12:46

S79	5	380/37,44,46,28.ccls. and (intermediate adj data) same (stage step) and (random adj number)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/06/08 12:47
S80	17	380/37,44,46,28.ccls. and (intermediate adj data) same (stage step)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/06/08 12:47

PORTAL USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ◉ The ACM Digital Library ○ The Guide

cryptanalysis, power, encryption, "intermediate data"

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used **cryptanalysis power encryption intermediate data** Found **2,277** of **156,259**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

☐ Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown Relevance scale

1 Technical opinion: designing cryptography for the new century

Susan Landau

May 2000 **Communications of the ACM**, Volume 43 Issue 5

Full text available: pdf(215.10 KB) html(35.06 KB) Additional Information: full citation, references, index terms

2 On the security of multiple encryption

Ralph C. Merkle, Martin E. Hellman

July 1981 **Communications of the ACM**, Volume 24 Issue 7

Full text available: pdf(269.82 KB) Additional Information: full citation, abstract, references, citings, index terms

Double encryption has been suggested to strengthen the Federal Data Encryption Standard (DES). A recent proposal suggests that using two 56-bit keys but enciphering 3 times (encrypt with a first key, decrypt with a second key, then encrypt with the first key again) increases security over simple double encryption. This paper shows that although either technique significantly improves security over single encryption, the new technique does not significantly increase security over simple doub ...

Keywords: DES, cipher, cryptanalysis, cryptography, data encryption standard, encipher, encrypt, encryption, multiple encryption

3 Power modeling and optimization for embedded systems: Analyzing the energy consumption of security protocols

Nachiketh R. Potlapally, Srivaths Ravi, Anand Raghunathan, Niraj K. Jha

August 2003 **Proceedings of the 2003 international symposium on Low power electronics and design**

Full text available: pdf(271.69 KB) Additional Information: full citation, abstract, references, citings, index terms

Security is critical to a wide range of wireless data applications and services. While several security mechanisms and protocols have been developed in the context of the wired Internet, many new challenges arise due to the unique characteristics of battery powered embedded systems. In this work, we focus on an important constraint of such devices -- battery life -- and examine how it is impacted by the use of security protocols.We present a

comprehensive analysis of the energy requirements of a ...

Keywords: 3DES, AES, DES, DSA, Diffie-Hellman, ECC, RSA, SSL, cryptographic algorithms, embedded system, energy analysis, handheld, low-power, security, security protocols

4 Concurrent error detection of fault-based side-channel cryptanalysis of 128-bit symmetric block ciphers

Ramesh Karri, Kaijie Wu, Piyush Mishra, Yongkook Kim

June 2001 **Proceedings of the 38th conference on Design automation**

Full text available: pdf(260.32 KB) Additional Information: full citation, abstract, references, index terms

Fault-based side channel cryptanalysis is very effective against symmetric and asymmetric encryption algorithms. Although straightforward hardware and time redundancy based concurrent error detection (CED) architectures can be used to thwart such attacks, they entail significant overhead (either area or performance). In this paper we investigate systematic approaches to low-cost, low-latency CED for symmetric encryption algorithms based on the inverse relationship that exists between encryp ...

5 Power Attack Resistant Cryptosystem Design: A Dynamic Voltage and Frequency Switching Approach

Shengqi Yang, Wayne Wolf, N. Vijaykrishnan, D. N. Serpanos, Yuan Xie

March 2005 **Proceedings of the conference on Design, Automation and Test in Europe - Volume 3**

Full text available: pdf(291.83 KB) Additional Information: full citation, abstract

A novel power attack resistant cryptosystem is presented in this paper. Security in digital computing and communication is becoming increasingly important. Design techniques that can protect cryptosystems from leaking information have been studied by several groups. Power attacks, which infer program behavior from observing power supply current into a processor core, are important forms of attacks. Various methods have been proposed to countermeasure the popular and efficient power attacks. Howe ...

6 Cryptanalysis of some encryption/cipher schemes using related key attack

Khawaja Amer Hayat, Umar Waqar Anis, S. Tauseef-ur-Rehman

June 2004 **ACM SIGCSE Bulletin , Working group reports from ITiCSE on Innovation and technology in computer science education**, Volume 36 Issue 4

Full text available: pdf(274.24 KB) Additional Information: full citation, abstract, references

This paper represents some Related Key attacks on the block ciphers like Biham-DES, DES-X, New DES and 3 way attacks. We will try to deal individual by adopting general attacking scheme. The paper also includes some suggestions to protect one from such attacks. Finally, the paper ends with the results.

Keywords: DES, cryptanalysis, differential related key attacks, related key attack

7 Design analysis techniques: Energy-aware design techniques for differential power analysis protection

Luca Benini, Alberto Macii, Enrico Macii, Elvira Omerbegovic, Fabrizio Pro, Massimo Poncino

June 2003 **Proceedings of the 40th conference on Design automation**

Full text available: pdf(286.41 KB) Additional Information: full citation, abstract, references, citings, index terms

Differential power analysis is a very effective cryptanalysis technique that extracts

information on secret keys by monitoring instantaneous power consumption of cryptoprocessors. To protect against differential power analysis, power supply noise is added in cryptographic computations, at the price of an increase in power consumption. We present a novel technique, based on well-known power-reducing transformations coupled with randomized clock gating, that introduces a significant amount of scra ...

Keywords: differential power analysis, low-power design

8 Differential cryptanalysis of hash functions based on block ciphers
Bart Preneel, Rene Govaerts, Joos Vandewalle
December 1993 **Proceedings of the 1st ACM conference on Computer and communications security**
Full text available: pdf(609.16 KB) Additional Information: full citation, abstract, references, index terms

This paper describes a differential attack on several hash functions based on a block cipher. The emphasis will be on the results for cases where DES [8] is the underlying block cipher. It will briefly discuss the case of FEAL-N [19, 21].

9 Security in embedded systems: Design challenges
Srivaths Ravi, Anand Raghunathan, Paul Kocher, Sunil Hattangady
August 2004 **ACM Transactions on Embedded Computing Systems (TECS)**, Volume 3 Issue 3
Full text available: pdf(3.67 MB) Additional Information: full citation, abstract, references, index terms, review

Many modern electronic systems---including personal computers, PDAs, cell phones, network routers, smart cards, and networked sensors to name a few---need to access, store, manipulate, or communicate sensitive information, making security a serious concern in their design. Embedded systems, which account for a wide range of products from the electronics, semiconductor, telecommunications, and networking industries, face some of the most demanding security concerns---on the one hand, they are oft ...

Keywords: Embedded systems, architecture, authentication, battery life, cryptographic algorithms, decryption, encryption, hardware design, processing requirements, security, security attacks, security protocols, tamper resistance

10 Security on FPGAs: State-of-the-art implementations and attacks
Thomas Wollinger, Jorge Guajardo, Christof Paar
August 2004 **ACM Transactions on Embedded Computing Systems (TECS)**, Volume 3 Issue 3
Full text available: pdf(296.79 KB) Additional Information: full citation, abstract, references, index terms

In the last decade, it has become apparent that embedded systems are integral parts of our every day lives. The wireless nature of many embedded applications as well as their omnipresence has made the need for security and privacy preserving mechanisms particularly important. Thus, as field programmable gate arrays (FPGAs) become integral parts of embedded systems, it is imperative to consider their security as a whole. This contribution provides a state-of-the-art description of security issues ...

Keywords: Cryptography, FPGA, attacks, cryptographic applications, reconfigurable hardware, reverse engineering, security

11 Designing encryption algorithms for real people
Bruce Schneier
August 1994 **Proceedings of the 1994 workshop on New security paradigms**

Full text available: pdf(332.46 KB) Additional Information: full citation, abstract, references, index terms

There is a wide disparity between cryptographic algorithms as specified by researchers and cryptographic algorithms as implemented in software applications. Programmers are prone to implement poor key management, make mistakes coding the algorithm, and use the algorithm in ways and for periods of time not originally intended. I propose design heuristics for designing algorithms in the "hostile" implementation environment of real-world software development. In the real ...

12 Security as a new dimension in embedded system design: Security as a new dimension in embedded system design

Srivaths Ravi, Paul Kocher, Ruby Lee, Gary McGraw, Anand Raghunathan

June 2004 **Proceedings of the 41st annual conference on Design automation - Volume 00**

Full text available: pdf(209.10 KB) Additional Information: full citation, abstract, references, citings, index terms

The growing number of instances of breaches in information security in the last few years has created a compelling case for efforts towards secure electronic systems. Embedded systems, which will be ubiquitously used to capture, store, manipulate, and access data of a sensitive nature, pose several unique and interesting security challenges. Security has been the subject of intensive research in the areas of cryptography, computing, and networking. However, despite these efforts, *security is* ...

***Keywords**: PDAs, architectures, battery life, cryptography, design, design methodologies, digital rights management, embedded systems, performance, security, security processing, security protocols, sensors, software attacks, tamper resistance, trusted computing, viruses*

13 Services: TinySec: a link layer security architecture for wireless sensor networks

Chris Karlof, Naveen Sastry, David Wagner

November 2004 **Proceedings of the 2nd international conference on Embedded networked sensor systems**

Full text available: pdf(316.88 KB) Additional Information: full citation, abstract, references, index terms

We introduce TinySec, the first fully-implemented link layer security architecture for wireless sensor networks. In our design, we leverage recent lessons learned from design vulnerabilities in security protocols for other wireless networks such as 802.11b and GSM. Conventional security protocols tend to be conservative in their security guarantees, typically adding 16--32 bytes of overhead. With small memories, weak processors, limited energy, and 30 byte packets, sensor networks cannot affo ...

Keywords: link layer security, sensor network security

14 Cryptology in Transition

Abraham Lempel

December 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 4

Full text available: pdf(1.63 MB) Additional Information: full citation, references, citings, index terms

15 Fast cache and bus power estimation for parameterized system-on-a-chip design

Tony D. Givargis, Frank Vahid, Jörg Henkel

January 2000 **Proceedings of the conference on Design, automation and test in Europe**

Full text available: pdf(86.67 KB) Additional Information: full citation, references, citings, index terms
Publisher Site

Keywords: cache, estimation, intellectual property, low power, on-chip bus, system-on-a-chip

16 Security evaluation of email encryption using random noise generated by LCG
Chung-Chih Li, Hema Sagar R. Kandati, Bo Sun
April 2005 **Journal of Computing Sciences in Colleges**, Volume 20 Issue 4
Full text available: pdf(153.28 KB) Additional Information: full citation, abstract, references

Theoretically, using any Linear Congruence Generator (LCG) to generate pseudo-random numbers for cryptographic purposes is problematic because of its predictableness. On the other hand, due to its simplicity and efficiency, we think that the LCG should not be completely ignored. Since the random numbers generated by the LCG are predictable, it is clear that we cannot use them directly. However, we shall not introduce too much complication in the implementation which will compromise the reasons, ...

Keywords: email encryption, lightweight encryptions, linear congruential generator

17 Cryptographic tools: Versatile padding schemes for joint signature and encryption
Yevgeniy Dodis, Michael J. Freedman, Stanislaw Jarecki, Shabsi Walfish
October 2004 **Proceedings of the 11th ACM conference on Computer and communications security**
Full text available: pdf(203.91 KB) Additional Information: full citation, abstract, references, index terms

We propose several highly-practical and optimized constructions for joint signature and encryption primitives often referred to as signcryption. All our signcryption schemes, built directly from trapdoor permutations such as RSA, share features such as simplicity, efficiency, generality, near-optimal exact security, flexible and ad-hoc key management, key reuse for sending/receiving data, optimally-low message expansion, "backward" use for plain signature/encryption, long messa ...

Keywords: extractable commitments, feistel transform, joint signature and encryption, signcryption, universal padding schemes

18 Symmetric and Asymmetric Encryption
Gustavus J. Simmons
December 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 4
Full text available: pdf(2.23 MB) Additional Information: full citation, references, citings, index terms

19 Design Method for Constant Power Consumption of Differential Logic Circuits
Kris Tiri, Ingrid Verbauwhede
March 2005 **Proceedings of the conference on Design, Automation and Test in Europe - Volume 1**
Full text available: pdf(146.44 KB) Additional Information: full citation, abstract

Side channel attacks are a major security concern for smart cards and other embedded devices. They analyze the variations on the power consumption to find the secret key of the encryption algorithm implemented within the security IC. To address this issue, logic gates

that have a constant power dissipation independent of the input signals, are used in security ICs. This paper presents a design methodology to create fully connected differential pull down networks. Fully connected differential pul ...

20 Some facets of complexity theory and cryptography: A five-lecture tutorial



Jörg Rothe
December 2002 **ACM Computing Surveys (CSUR)**, Volume 34 Issue 4

Full text available: pdf(2.78 MB) Additional Information: full citation, abstract, references, citings, index terms, review

In this tutorial, selected topics of cryptology and of computational complexity theory are presented. We give a brief overview of the history and the foundations of classical cryptography, and then move on to modern public-key cryptography. Particular attention is paid to cryptographic protocols and the problem of constructing key components of protocols such as one-way functions. A function is one-way if it is easy to compute, but hard to invert. We discuss the notion of one-way functions both ...

Keywords: Complexity theory, interactive proof systems, one-way functions, public-key cryptography, zero-knowledge protocols

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2005 ACM, Inc.
Terms of Usage Privacy Policy Code of Ethics Contact Us

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player